IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

I hereby certify that this paper is beingdeposited on this date with the U.S. Postal Service as first class mail addressed to the Commissionerfor Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: ______________ Date: November 21, 2005

Applicant(s):	B.M. Jakobsson et al.
Case:	22-2
Serial No.:	09/538,663
Filing Date:	March 30, 2000
Group:	3624
Examiner:	Stefanos Karmis

Title: Methods of Protecting Against Spam Electronic Mail

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter referred to as "Appellants") hereby appeal the final rejection of claims 1-6, 8-13 and 15-20 of the above referenced application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc. The assignee Lucent Technologies Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

Claims 1-6, 8-13 and 15-20 are pending in the present application. Claims 1-6, 8-13 and 15-20 stand rejected under 35 U.S.C. §103(a) and are appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates generally to methods for controlling incoming or received electronic mail (email). More specifically, the invention relates to methods for protecting against the receipt of unwanted or "spam" email in a telecommunication system. See page 2, lines 3-5 of the Specification.

Claim 1 provides a method for preventing receipt by receivers of unwanted email sent by senders in a communication system. It is determined whether email to a receiver comprises valid message authentication code (MAC) information. Email directed to the receiver that does not comprise valid MAC information is filtered out at a gateway of the communication system. The receiver is provided with email directed to the receiver that comprises valid MAC information. Independent claim 10 recites another aspect of the present invention having similar limitations.

By way of example, an illustrative embodiment of the invention of claim 1 is shown in FIG. 2 of the drawings. FIG. 2 is a flow chart of a preferred method of preventing the undesired receipt of spam email. At step 140, it is determined whether the email is valid according to a processed MAC. It is preferable to determine an extension of the receiver's email address such that when this extension appears in the email, the receiver will accept the email. The email is accepted at step 150 if and only if the same extension of the receiver's address is the same as a result calculated for the extension. Otherwise the email is refused at step 160. See page 14, lines 1-12 of the Specification.

Claim 2 provides a method as in claim 1, further comprising the step of registering a sender. A cookie is established by the sender which indicates to the receiver whether the sender has satisfied the requirement to allow the sender to become a registered sender to the receiver. An address related to an address associated with the receiver is established which will inform the sender that the receiver desires that the sender be able to send email to the receiver. A key is established by the receiver which is forwarded to the sender by the receiver to inform the sender that the sender is authorized to send email to the receiver and is now a registered sender. The key is also for use by the sender whenever the sender wishes to send email to the receiver.

By way of example, an illustrative embodiment of the invention of claim 2 is shown in FIG. 2 of the drawings. The sender sets up a cookie using a stream cipher generated pad at step 110 and sends it to the receiver so that the receiver can decide whether it wishes to receive email from this sender. The receiver then verifies the correctness of the cookie and, at step 120, selects a symmetric key, uniformly at random from a set of possible keys at the receiver's disposal. After the symmetric key is selected by the receiver, the receiver preferably adds redundancy to the key by replying to the sender using a public extension on the receiver's address appended solely for the purpose of setup. The sender then stores the key in a list of all such access keys, thereby allowing future emails from the sender to the receiver to be processed using this key. See page 12, line 1 through page 13, line 10 of the Specification.

The methods of preventing spam email in accordance with the present invention are efficient and computationally non-intensive, thereby conserving the resources of the communication system. Moreover, the inventive methods provide authenticity verification of the email with very little extra computation costs. Additionally, the methods of the present invention achieve message privacy using standard encryption methods and successfully manage data transmission problems associated with sending sensitive information by email. Such features, benefits and advantages have not heretofore been achieved in the art. See page 5, lines 16-22 of the Specification.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-6, 8-13 and 15-20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,199,102 (hereinafter "Cobb") in view of U.S. Patent No. 6,640,301 (hereinafter "Ng").

ARGUMENT

Appellants incorporate by reference herein the disclosures of all previous responses filed in the present application, namely, responses dated June 24, 2004, January 26, 2005 and August 17, 2005.

A. Claims 1, 8-13, 15-20

Regarding the §103(a) rejection based on a combination of Cobb and Ng, Appellants respectfully assert that the cited combination fails to establish a prima facie case of obviousness under 35 U.S.C. §103(a), as specified in M.P.E.P. §2143.

As set forth therein, M.P.E.P. §2143 states that three requirements must be met to establish a prima facie case of obviousness. First, the cited combination must teach or suggest all the claim limitations. Second, there must be a reasonable expectation of success. Third, there must be some suggestion or motivation to combine reference teachings. While it is sufficient to show that a prima facie case of obviousness has not been established by showing that one of the requirements has not been met, Appellants respectfully believe that none of the requirements have been met.

First, with respect to independent claims 1 and 10, the collective teaching of Cobb and Ng fails to suggest or render obvious the elements of such claims. For at least this reason, a prima facie case of obviousness has not been established.

Cobb discloses a method and system for filtering electronic messages. A message is received from a sender, a challenge is sent back the sender, a response to the challenge is received, and it is determined if the response is proper. In rejecting the claims, the Examiner refers to portions of Cobb regarding address verification and the providing of a "challenge" to an unrecognized sender. However, with regard to independent claims 1 and 10, Cobb fails to disclose a determination of whether email to a particular receiver comprises valid message authentication code (MAC) information. Cobb further fails to disclose that email directed to the particular receiver that does not comprise valid MAC information is filtered out at a gateway of the communication system. Cobb contains no disclosure of MAC information and fails to disclose or suggest the utilization of MAC information in preventing receipt of unwanted email in a communication system.

Ng discloses a third-party email authentication service provider. In rejecting the claims, the Examiner refers to portions of Ng that address authentication of email messages through the sending of a copy of the received email message to an authentication service. In Ng, no filtering occurs since the receiver would have already received the email message before it is sent for authentication. Ng fails to remedy the deficiencies described above with regard to Cobb. Ng also contains no disclosure or suggestion to utilize MAC information in preventing receipt of unwanted email in a communication system. The combination of Cobb and Ng fails to disclose that email directed to the particular receiver that does not comprise valid MAC information is filtered out at a gateway of the communication system.

Second, with respect to claims 1 and 10, Appellants assert that there is no reasonable expectation of success in achieving the present invention through a combination of Cobb and Ng. For at least this reason, a prima facie case of obviousness has not been established.

Despite the assertion in the final Office Action, Appellants do not believe that Cobb and Ng are combinable since it is not clear how one would combine them. Cobb filters messages before they are received by the email receiver based on a challenge answer sent by the email sender, while Ng authenticates email messages that have already been received by the email receiver. Cobb filters email messages so that only authentic messages are received by the receiver, therefore an authentication system as described in Ng is not required. No guidance was provided in the final Office Action as to how the two references can be combined to achieve the present invention. However, even if combined, for the sake of argument, they would not achieve the techniques of the claimed invention as described above.

Third, with respect to claims 1 and 10, Appellants assert that no motivation or suggestion exists to combine Cobb and Ng in a manner proposed by the Examiner, or to modify their teachings to meet the claim limitations. For at least this reason, a prima facie case of obviousness has not been established.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id at 1343-1344.

With regard to claims 1 and 10, in the final Office Action, in section 7 on pages 6-7, the Examiner provides the following statement to prove motivation to combine Cobb and Ng:

> It would have been obvious . . . to modify the teachings of Cobb and include the teachings of Ng and have the email authenticated with codes because it provides a form of filtering based on an attribute associated with an email, so that fraudulent or unwanted emails can be screened.

The Examiner's conclusory statement does not adequately address the issue of motivation to combine references, and Appellants submit that this statement is based on the type of "subjective belief and unknown authority" that the Federal Circuit has indicated provides insufficient support for an obviousness rejection. Additionally, the Examiner fails to identify any objective evidence of record which supports the proposed combination.

It is well-settled law that "teachings of references can be combined *only* if there is some suggestion or incentive to do so." *ACS Hosp. Sys. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984) (emphasis in original). Moreover, in order to avoid the improper use of a hindsight-based obviousness analysis, particular findings must be made as to why one skilled in the relevant art, having no knowledge of the claimed invention, would have selected the components disclosed by Cobb and Ng in the manner claimed (*See, e.g.*, *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000)). No such findings have been provided in the final Office Action. "It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" *In re Sang-Su Lee*, 277 F.3d 1338, 1344 (Fed. Cir. 2002) (quoting *W.L. Gore v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983)).

Dependent claims 8, 9, 11-13 and 15-20 are patentable at least by virtue of their dependency from independent claims 1 and 10. The patentability of independent claims 1 and 10 is described above. Dependent claims 8, 9, 11-13 and 15-20 also recite patentable subject matter in their own right.

Appellants further assert that the Ng reference is not valid prior art. In a response to an Office Action filed on June 24, 2004, a declaration under 37 C.F.R. §1.131 was submitted establishing a conception date for the present invention at least as early as April 2, 1999, and due diligence until filing of the application on March 30, 2000. The Examiner indicated that the filed declaration was acceptable in an Office Action sent on September 29, 2004.

A disclosure relating to the present invention was sent to outside patent counsel for preparation and filing of a patent application on May 21, 1999. Outside patent counsel provided a draft patent application to the inventors for their review on October 15, 1999. Multiple series of comments and draft applications were provided in the following months until a finalized application was filed on March 30, 2000. Appellants and those involved in preparing and filing the subject application on Appellant's behalf, exercised reasonable diligence from April 2, 1999 up to the filing date of the application as is evident from the submitted declaration.

Thus, while Appellants assert that claims 1, 8-13 and 15-20 are patentable over the combination of Cobb and Ng for the reasons provided above, Appellants again request removal of the Ng reference as prior art. Therefore, for at least the reasons given above, Appellants respectfully request that the §103(a) rejection of claims 1, 8-13 and 15-20 be withdrawn.

B. Claims 2-6

Dependent claim 2 is patentable at least by virtue of its dependency from independent claim 1. The patentability of claim 1 is described above. However, dependent claim 2 also recites patentable subject matter in its own right.

While Cobb discloses the use of an acceptance list and the registration of users on the acceptance list, Cobb fails to disclose the establishment of an address related to an address associated with the receiver which will inform the sender that the receiver desires that the sender be able to send email to the receiver. Cobb also fails to disclose the establishment by the receiver of a key which is forwarded to the sender by the receiver to inform the sender that the sender is authorized to send email to the receiver and is now a registered sender and for use by the sender whenever the sender wishes to send email to the receiver.

Dependent claims 3-6 are patentable at least by virtue of their dependency from dependent claim 2. The patentability of dependent claim 2 is described above. Dependent claims 3-6 also recite patentable subject matter in their own right. Therefore, for at least the reasons given above, Appellants respectfully request that the §103(a) rejection of claims 2-6 be withdrawn.

For at least the reasons given above, Appellants respectfully request withdrawal of the §103(a) rejection of claims 1-6, 8-13 and 15-20. Appellants believe that claims 1-6, 8-13 and 15-20 are patentable over the combination of Cobb and Ng. As such, the application is believed to be in condition for allowance, and favorable action is respectfully solicited.

Respectfully submitted,

Robert W. Griffith

Date: November 21, 2005

Robert W. Griffith
Attorney for Applicant(s)
Reg. No. 48,956
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-4547

CLAIMS APPENDIX

1. A method for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising the steps of:

determining whether email to a particular receiver comprises valid message authentication code (MAC) information;

filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information; and

providing the particular receiver with email directed to the particular receiver that comprises valid MAC information.

2. The method of claim 18, wherein the step of registering the particular sender comprises the steps of:

establishing by the particular sender a cookie which indicates to the particular receiver whether the particular sender has satisfied the requirement to allow the particular sender to become a registered sender to the particular receiver;

establishing an address related to an address associated with the particular receiver which will inform the particular sender that the particular receiver desires that the particular sender be able to send email to the particular receiver; and

establishing by the particular receiver a key which is forwarded to the particular sender by the particular receiver to inform the particular sender that the particular sender is authorized to send email to the particular receiver and is now a registered sender and for use by the particular sender whenever the particular sender wishes to send email to the particular receiver.

3. The method recited in claim 2, wherein said step of establishing the address comprises generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

4. The method recited in claim 2, wherein said step of establishing an address comprises sending email from the particular receiver to the particular sender using public key encryption.

5. The method recited in claim 2, wherein said registering step further comprises sending to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

6. The method recited in claim 5, further comprising the step of storing the encrypted key by the particular sender in a table of encrypted keys for use by the particular sender whenever the particular sender desires to send email to the particular receiver.

8. The method of claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC against a value determined by the particular receiver.

9. The method recited in claim 1, wherein the step of determining whether email comprises valid MAC information comprises comparing the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

10. A server for preventing receipt by receivers of unwanted electronic mail messages (email) sent by senders in a communication system, comprising:

a determining module for determining whether email to a particular receiver comprises valid message authentication code (MAC) information;

a filtering module for filtering out at a gateway of the communication system email directed to the particular receiver that does not comprise valid MAC information; and

a provisioning module for providing the particular receiver with email directed to the particular receiver that comprises valid MAC information.

11. The server recited in claim 20, wherein said registering module further comprises a generator for generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver.

12. The server recited in claim 11, wherein said registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption.

13. The server recited in claim 11, wherein said registering module sends to the particular user by the particular receiver, an encrypted key wherein the encrypted key is a member of a set of encrypted keys.

15. The server of claim 10, wherein said filtering module compares the MAC against a value.

16. The server recited in claim 15, wherein the filtering module compares the MAC to an available header in an address of the particular receiver, in the received email message, whereby the MAC is not a valid MAC if the MAC and the header are not identical.

17. The method of claim 1, further comprising the step of determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement.

18. The method of claim 17, further comprising the step of registering the particular sender when the particular sender is determined not to be a registered send of email to the particular receiver.

19. The server of claim 10, further comprising a registering module for determining if a particular sender is a registered sender of email to the particular receiver, wherein the particular sender becomes a registered sender by satisfying a requirement.

20. The server of claim 19, wherein the registering module is also for registering the particular sender when the particular sender is determined not to be a registered send of email to the particular receiver.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.